

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA )  
v. )  
JASON JIMENEZ, )  
Defendant. )  
Crim. No. 19-10278-RWZ

**GOVERNMENT'S OPPOSITION TO DEFENDANT'S MOTION TO COMPEL  
ACCESS TO SEIZED MOBILE PHONE AND GOVERNMENT'S  
MOTION TO COMPEL PASSCODE TO MOBILE PHONE**

The United States respectfully opposes Defendant Jason Jimenez (“Jimenez”)’s motion to compel “limited access” to the Apple iPhone that law enforcement agents lawfully seized at the time of Jimenez’s arrest. Jimenez’s request aims to effect an end-run around a search warrant, which the Court (Hennessy, M.J.) lawfully issued, but from which the government has not yet been able to retrieve any evidence. The Court should deny Jimenez’s motion.

Separately, because Jimenez has conceded his ability to access the iPhone, the Court should issue an order under the All Writs Act, compelling Jimenez to produce his passcode to the government.

## BACKGROUND

The government’s allegations are contained within the Affidavit of Keith Weidlich in support of a Criminal Complaint (“Compl.”), *see* ECF No. 1-1. The government briefly summarizes those allegations that are relevant to Jimenez’s motion here:

On July 10, 2019, law enforcement officers observed Jimenez's conduct what they believed to be a sale of narcotics in Lawrence, Massachusetts. Compl. ¶¶ 6-9. After making this observation, the officers followed the car that Jimenez was driving. They then observed what they believed to be Jimenez attempting to secrete contraband in his car. *Id.* Ultimately, officers initiated a traffic stop of Jimenez's car. *Id.* ¶¶ 14-15. After initiating the traffic stop, law enforcement advised Jimenez of his *Miranda* rights and informed Jimenez that they were investigating suspected narcotics activity. *Id.* ¶¶ 17-18.

After officers advised Jimenez of his *Miranda* rights, Jimenez asked to use his Apple iPhone to record his interactions with the officers. *Id.* ¶ 17. Jimenez then activated the recording function on his iPhone. *Id.* After Jimenez activated the iPhone, the officers asked Jimenez a series of questions regarding a passenger that they had observed briefly riding in Jimenez's car. *Id.* ¶ 18-19. Officers believe that this passenger purchased illegal narcotics from Jimenez. After Jimenez offered a series of inconsistent answers to officers' questions, the officers asked Jimenez to exit his car. *Id.* ¶ 20. Jimenez did not take his iPhone with him when he exited the vehicle.

Once Jimenez was out of the vehicle and he was separated from his iPhone, officers conducted a pat frisk in which they discovered a bulge that they believed to be illicit narcotics. *Id.* ¶ 21. When officers confronted Jimenez about the bulge and suggested that he was involved in the sale of illegal narcotics, Jimenez responded, "yeah, yeah, yeah, it is what it is." *Id.* ¶ 22. Officers then removed substances from Jimenez's underwear that the DEA lab later concluded were fentanyl and crack cocaine. The officers then placed Jimenez under arrest. *Id.* Among other things, the officers seized Jimenez's iPhone.

After his arrest, the Court (Hennessy, M.J.) issued a warrant to search the iPhone for evidence of possession and distribution of controlled substances; evidence of user attribution; and records of internet use. *See* ECF No. 34-1 at 5-6. The FBI took custody of the iPhone and attempted to execute the warrant, but was unable to access the phone's contents at the Regional Computer Forensics Laboratory, as it cannot currently defeat the lock feature. However, the FBI does have access to additional technological solutions at other facilities, and may be able to access the phone at those facilities. More importantly, historically the FBI has ultimately been able to access the contents of most iPhone devices, as the technology is updated to adapt to each new operating system. Thus, with additional time and/or resources, the FBI anticipates that it will be able to unlock the device.

## ARGUMENT

**I. JIMENEZ'S MOTION DOES NOT SEEK AN ORDER COMPELLING PRODUCTION OF EVIDENCE TO WHICH THE GOVERNMENT LACKS ACCESS, BUT INSTEAD SEEKS THE RETURN OF SEIZED PROPERTY**

Although Jimenez has styled his motion as a motion to compel access to a video recording, the government lacks access to the video recording contained within the iPhone. The government cannot produce information that is not in its possession. *United States v. Canniff*, 521 F.2d 565, 573 (2d Cir.), *cert. denied*, 423 U.S. 1059 (1975) (“Clearly the government cannot be required to produce that which it does not control and it never possessed or inspected.”). In actuality, Jimenez’s motion seeks the return of property, pursuant to Fed. R. Crim. P. 41(g). As discussed further below, under that standard, Jimenez’s motion should fail.

## II. THE COURT SHOULD NOT RETURN JIMENEZ'S PROPERTY

### A. Jimenez Cannot Satisfy His Burden to Compel the Return of Seized Property, Which Continues to Have Evidentiary Value to the Government

Jimenez cannot satisfy his burden to compel the return of his property under Rule 41(g).

That rule provides that a person “aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property’s return.” When criminal charges are pending, the defendant bears the burden of proving that he is entitled to lawful possession of the property. *See United States v. Clifford*, 297 F. Supp. 2d 308, 310 (D. Me. 2003) (citing *United States v. Chambers*, 192 F.3d 374, 377 (3rd Cir. 1999); *United States v. Martinson*, 809 F.2d 1364, 1369 (9th Cir. 1987). Once the property “is no longer needed for evidentiary purposes,” the burden of proof shifts. *Martinson*, 809 F.2d at 1369. The ostensible reason being, where criminal proceedings remain pending, the government’s interest in the evidentiary value of seized property outweighs the defendant’s property interest. *See United States v. Pierre*, 484 F.3d 75, 87 (1st Cir. 2007) (“[A] Rule 41(g) motion is properly denied if the defendant is not entitled to lawful possession of the seized property, the property is contraband or subject to forfeiture, or the government’s need for the property as evidence continues.”) (citation, internal quotation marks, and alterations omitted).

Here, the government is entitled to lawful possession of the iPhone it seized. After officers arrested Jimenez, a valid warrant issued for the search of the iPhone. Although the government has not yet successfully decrypted the iPhone, the evidentiary value that formed the basis of the warrant is exactly the same as it was when the warrant issued: there is evidence, fruits and instrumentalities of the crime, contained on the device. The defendant concedes as

much. And the government will eventually be able to access what it has rightful authority to search. Each time Apple has released a new operating system for iPhones, FBI has eventually developed to new technologies to decrypt iPhones using the new operating system. It is therefore likely only a matter of time until FBI develops technology to decrypt Jimenez's iPhone. *See United States v. Pinto-Thomaz*, 352 F. Supp. 3d 287, 312-13 (S.D.N.Y. 2018) (denying defendant's motion to return iPhone where the government "continues to need the iPhone for its preparation for trial and continues to seek to de-encrypt the iPhone as it accesses new technology. . . . As the Government has been unable to access and image the contents of the iPhone, its interests would be sacrificed by the phone's return."). The Court should not force the government to return property that contains evidence relevant to the government's case.

B. The Government's Return of Property to Jimenez Would Destroy the Property's Evidentiary Value

Were the Court to order that the government return the iPhone to Jimenez, this would have adverse consequences on the evidentiary value of the device. The government would not be able to present witnesses establishing that any information it subsequently extracts from the iPhone is authentic. "When evidence . . . is susceptible to alteration, the proponent of the evidence must establish a chain of custody to render it improbable that the original item has been exchanged, tampered with, or contaminated." *United States v. Barandica*, 960 F.2d 143 (unpublished), No. 91-1511, 1992 WL 75138, at \*3 (1st Cir. 1992). The government's surrender of the iPhone to Jimenez would also provide him with an opportunity to tamper with, destroy, or alter evidence contained within the iPhone. This would be analogous to agents securing a defendant's home to conduct a search, but allowing the defendant to go back inside

the home before the search was conducted. The government's surrender of the device would, at best, raise questions about the authenticity of evidence the government subsequently extracts and seeks to admit, or at worst, raise concerns about whether the government was deprived of an opportunity to discover relevant evidence within the scope of its search warrant.

Although Jimenez suggests that the Court could order the government to turn over the iPhone to a "neutral third party vendor," doing so would not ameliorate the government's concerns about later establishing chain-of-custody. Nor is it a precedent the government believes is prudent or appropriate. Law enforcement agents that execute search warrants on electronic devices are forensically trained agents with technical skills and a sworn duty, who are trained to handle evidence and prepared to testify about the process. This is not a task that can or should be handled by a private vendor.

Moreover, Jimenez's suggestion that the third party vendor be used is itself significant. Jimenez's engagement of a third-party would require Jimenez to provide his passcode to the third-party. In doing so, Jimenez would moot his constitutional objections (Jimenez Motion, ECF No. 34 at 4) to the government's request that he provide his passcode to the government, as the passcode would now be in the possession of the third-party, from whom the government could compel its production.<sup>1</sup>

---

<sup>1</sup> As discussed further below, the government requests that the Court order Jimenez to produce his passcode to the government.

C. The Government’s Refusal to Return of Jimenez’s Does Not Deprive Him of His Constitutional Right to Exculpatory Evidence

Jimenez’s assertions that the iPhone *may* contain exculpatory evidence does not compel the Court to order the iPhone’s return. “A defendant’s right to discover exculpatory evidence does not include the unsupervised authority to search through the [government’s] files” or the authority to decide materiality “alone.” *Pennsylvania v. Ritchie*, 480 U.S. 39, 59-60 (1987). Instead, “it is the [government] that decides which information must be disclosed.” *Id.* at 60; *see also Weatherford v. Bursey*, 429 U.S. 545, 559 (1977) (“There is no general constitutional right to discovery in a criminal case, and *Brady* did not create one.”). Yet unsupervised access is precisely what Jimenez suggests.

**III. THE COURT SHOULD COMPEL JIMENEZ TO PROVIDE HIS PASSCODE TO THE GOVERNMENT**

The Court has the authority to issue an order compelling Jimenez to decrypt the iPhone. Where, as here, the court has the authority to issue a search warrant, it therefore has jurisdiction to issue an order under the All Writs Act, 28 U.S.C. § 1651(a), to ensure that the warrant can be executed. *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172 (1977) (recognizing “the power of a federal court to issue such commands under the All Writs Act as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained”). The All Writs Act extends to orders for decryption of electronic media. *See United States v. Apple MacPro Computer*, 851 F.3d 238, 245 (3d Cir. 2017) (affirming decryption order issued under the All Writs Act). The Court should therefore issue such an order here, to avoid frustration of a validly issued search warrant.

The Court should compel Jimenez to produce his passcode to the government, because any testimonial aspect of this production is a “foregone conclusion.” Jimenez cites *In re Grand Jury Subpoena Duces Tecum* for the proposition that “the decryption [of his iPhone] and production [of his passcode] would be tantamount to testimony . . . of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives, and of his capability to decrypt the files.” 670 F.3d 1335, 1346 (11th Cir. 2012). In other words, Jimenez asserts that the “act of production” of his passcode would be, in and of itself, incriminating. *See Fisher v. United States*, 425 U.S. 391, 408.

Here, however, an exception to the “act of production” doctrine, the “foregone conclusion” doctrine applies. Under the “foregone conclusion” doctrine, “the Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production such as the existence, custody, and authenticity of evidence—is a ‘foregone conclusion’ that ‘adds little or nothing to the sum total of the Government's information.’” *Apple MacPro Computer*, 851 F.3d at 247 (quoting *United States v. Hubbell*, 530 U.S. 27, 30 (2000)). By offering to provide his passcode to a “neutral third party vendor,” Jimenez has conceded that he possesses the passcode, and thus rendering any “testimony” that he has possess, control, access, and the ability to decrypt the iPhone a “foregone conclusion.” *See Apple MacPro Computer*, 851 F.3d at 248 (affirming district court’s order compelling production where it was undisputed that, prior to the seizure of certain computers, the target of a grand jury investigation “[u]nlike *In re Grand Jury Subpoena*, the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that [the recipient of a

decryption order] can access them"). In essence, Jimenez has already confirmed any testimonial information that he could provide by producing his passcode. The Court should therefore order Jimenez to decrypt his iPhone by providing the government with the passcode.

### **CONCLUSION**

For the foregoing reasons, the United States respectfully requests that the Court deny Jimenez's motion, and instead, order Jimenez to produce his iPhone's passcode to the government.

Respectfully submitted,

ANDREW E. LELLING  
UNITED STATES ATTORNEY

Dated: December 4, 2019

/s/ Evan D. Panich

Evan D. Panich, BBO #681730  
Assistant United States Attorney  
United States Attorney's Office  
1 Courthouse Way, Suite 9200  
Boston, MA 02210  
(617) 748-3652  
[evan.panich@usdoj.gov](mailto:evan.panich@usdoj.gov)

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

*/s/ Evan D. Panich* \_\_\_\_\_

Evan D. Panich  
Assistant U.S. Attorney

Date: December 4, 2019